# REMARKS

**[0002]** Applicant respectfully requests reconsideration and allowance of all of the claims of the application. The status of the claims is as follows:

- Claims 1-13, 19-29 and 31-40 are currently pending,
- No claims are canceled herein,
- No claims are withdrawn herein,
- Claim 1 is amended herein,
- No new claims are added herein.

## Claims Rejected Under § 101

**[0003]** Claims 1-12 stand rejected under 35 U.S.C. § 101 as allegedly being directed to non-statutory subject matter. Applicant respectfully traverses this rejection.

**[0004]** Nevertheless, Applicant amends claim 1 herein to address the rejection made by the Examiner. Applicant submits the rejection of these claims is rendered moot at least because of the amendment made herein.

## Cited Document

**[0005]** The Examiner's rejections are based upon the following reference:

- **Sankar**: Sankar, U.S. Patent No. 7,065,706.

**[0006]** Sankar is directed to a network router in an open protocol network. The disclosed router is described as being configured for executing network operations (e.g. routing requests and responses) for network nodes utilizing XML.

## Claims Rejected Based on Sankar

**[0007]** Claims 1-13, 19-29 and 31-40 stand rejected under 35 U.S.C. § 102(e) as allegedly being anticipated by Sankar. Applicant respectfully traverses the rejection.

*Independent Claim 1*

**[0008]** Applicant submits that the Office has not shown that Sankar anticipates this claim, as Sankar does not disclose at least the following features of this claim (with emphasis added):

- "***selecting a first set of security information*** from a first plurality of sets of security information as a function of a property of the message, **wherein the first set of security information comprises security settings**;"
- "***selecting a second set of security information*** from a second plurality of sets of security information as a function of the first set, wherein the second set of security information comprises security settings;"

**[0009]** The Examiner indicates (Action, pp. 4-5) the following with regard to this claim:

> Regarding claim 1, Sankar discloses:
>
> A method, comprising:
>
> on a device configured to receive messages, receiving a message (column 2, lines 35-39: *received message*);
>
> selecting a first set of security information (column 2, lines 25-35: *parsing XML tags to get information*) from a first plurality of sets of security information (column 2, lines 25-35: *XML tags*) as a function of a property of the message (column 2, lines 25-40: *wherein the message is received and then the XML tags are parsed*);
>
> selecting a second set of security information (column 2, lines 35-40: *retrieving the attributes (second set of security information) from the XML tags and determining identifying relevant attributes (selecting second set))* from a second plurality of sets of security information (column 2, lines 35-40: *retrieving all the attributes*) as a function of

the first set (column 2, lines 24-48: *wherein the attributes are retrieved by parsing the XML tags*); and

applying the second set of security information to the message (column 2, lines 43-46; *determining security attributes to determine the operation to be performed on the message*).

**[0010]** As can be seen, the Examiner equates the "XML tags" disclosed by Sankar with the claimed "first set of security information" and the "attributes" disclosed by Sankar as being equivalent to the claimed "second set of security information". Applicant respectfully disagrees.

**[0011]** While it is true that Sankar discloses that one of the attributes of a message can be "security attributes" (Col. 2, line 46), according to Sankar the XML tags are merely a container for attributes. Sankar expressly states "[t]he router includes an XML parser configured for parsing XML tags specifying prescribed attributes..." (Col. 2, ll. 28-29). The "XML tags" and the "attributes" are therefore not a first and second set of security information.

**[0012]** The claim expressly recites "selecting a first set of security information from a first plurality of sets of security information" and "selecting a second set of security information from a second plurality of sets of security information".

**[0013]** Since Sankar at best only discloses one set of security information; namely "security attributes", it can not be fairly said that Sankar anticipates this claim, for at least this reason.

**[0014]** Furthermore, the claim expressly recites that the selection is "from a first *plurality* of sets of security information". At best, Sankar only discloses a *singular* set of security information, therefore it would be impossible to select from a *plurality* of sets.

**[0015]** Applicant additionally notes that the claim recites "wherein the first set of security information comprises security settings". Here a second distinction exits because not only are the XML tags of Sankar not security information, they are not described as being security information comprised of security settings. The XML tags described by Sankar are merely containers for "security attributes". Applicant notes that the rejection does not appear to address the claimed features fully, and that the telephone call placed to the Examiner 06/30/09, to get clarification of the rejection, did not avail the applicant.

**[0016]** Accordingly, Applicant asks the Examiner to withdraw the rejection of this claim.

*Dependent Claims 2-13*

**[0017]** These claims ultimately depend upon independent claim 1. As discussed above, claim 1 is allowable. It is axiomatic that any dependent claim, which depends from an allowable base claim, is also allowable. Additionally, some or all of these claims may also be allowable for additional independent reasons.

*Independent Claim 19*

**[0018]** Applicant submits that the Office has not shown that Sankar anticipates this claim, as Sankar does not disclose at least the following features of this claim (with emphasis added):

- a first datastore to include ***a first plurality of sets of security settings*** related to an application residing in the system, wherein the first plurality of sets define messages that must be secured;
- a second datastore to include ***a second plurality of sets of security settings***, wherein the second plurality of sets specify settings and operations for securing messages, and wherein a set of the first plurality of sets is associated with a set of the second plurality of sets;

**[0019]** The Examiner indicates (Action, pp. 9-10) the following with regard to this claim:

Regarding claim 19, Sankar discloses:

A system comprising:

a processor (column 4, lines 8-15);

a memory coupled to the processor to store at least a portion of a plurality of datastores (column 4, lines 8-15);

a first datastore to include a first plurality of sets of security information (column 2, lines 25-35: *parsing XML tags to get information*) related to an application residing in the system (column 2, lines 25-40: *wherein the message is received and then the XML tags are parsed to determine which application/process the message is to be re-routed to*);

a second datastore to include a second plurality of sets of security information (column 2, lines 35-40: *retrieving the attributes (second set of security information)*, wherein a set of the first plurality of sets is associated with a set of the second plurality of sets (column 2, lines 24-48: *wherein the attributes are retrieved by parsing the XML tags*); and

a module to select a first set from the first plurality of sets as a function of a property of a received message (column 2, lines 25-40: *wherein the message is received and then the XML tags are parsed*).

**[0020]** Here, as can be seen, the Examiner asserts that because the XML tags are described as being parsed to determine routing information and security attributes, that this constitutes the claimed first and second plurality of sets of security "information". Applicant respectfully disagrees. Applicant reiterates that the reference does not describe a "a second plurality of sets of security settings".

**[0021]** Applicant notes that Sankar is directed to a network router for use in an open protocol network. The disclosed router is described as being configured for executing network operations (e.g. routing requests and responses) for network nodes utilizing XML (Sankar, Field of the Invention).

**[0022]** Sankar discloses that such a router must be capable of parsing XML messages (Col. 2, ll. 24-28). In describing the particular need for the router's XML parsing features, Sankar describes the need to identify the relevant attributes of a message such as a "security attribute" in order to perform certain operations.

**[0023]** As such, Sankar is only loosely related to the instant application, which "relates generally to security systems for computing environments" (Application, p. 1 "Field").

**[0024]** Furthermore, Sankar does not disclose, either expressly or impliedly, a plurality of ***sets*** of security settings.

**[0025]** Further still, it appears the Examiner is not rejecting all of the language currently recited in this claim. The rejection refers to "security information" yet the claim specifically recites "security settings".

**[0026]** For this and the forgoing reasons, Sankar does not disclose all of the elements and features of this claim. Accordingly, Applicant asks the Examiner to withdraw the rejection of this claim.

*Dependent Claims 20-29*

**[0027]** These claims ultimately depend upon independent claim 19. As discussed above, claim 19 is allowable. It is axiomatic that any dependent claim, which depends from an allowable base claim, is also allowable. Additionally, some or all of these claims may also be allowable for additional independent reasons.

*Independent Claim 31*

**[0028]** Applicant submits that the Office has not shown that Sankar anticipates this claim, as Sankar does not disclose the following features of this claim (with emphasis added):

- steps for selecting ***a first set of security information from a first plurality of sets of security information*** as a function of a property of the message, wherein the first set of security information comprises

security settings that define types of messages that must be secured and wherein the types of messages that must be secured are defined and provided by an application developer;

- steps for ***selecting a second set of security information from a second plurality of sets of security information*** as a function of the first set, wherein the second set of security information comprises security settings that specify particular operations and settings for securing the messages, wherein the particular operations and settings comprise algorithms to be used in signing and encrypting the messages; and
- ***steps for applying the second set of security information*** to the message.

**[0029]** The Examiner indicates (Action, pp. 12-13) the following with regard to this claim:

> Regarding claim 31, Sankar discloses:
>
> A machine-readable medium having components, comprising:
>
> steps for receiving a message (column 2, lines 35-39: *received message*);

steps for selecting a first set of security information (column 2, lines 25-35: *parsing XML tags to get information*) from a first plurality of sets of security information (column 2, lines 25-35: *XML tags*) as a function of a property of the message (column 2, lines 25-40: *wherein the message is received and then the XML tags are parsed*), wherein the first set of security information comprises security settings that define types of messages that must be secured and wherein the types of messages that must be secured are defined and provided by an application developer (column 2, lines 25-35: *parsing XML tags to get information about what security functions to perform on the message*);

steps for selecting a second set of security information (column 2, lines 35-40: *retrieving the attributes (second set of security information) from the XML tags and determining identifying relevant attributes (selecting second set)*) from a second plurality of sets of security information (column 2, lines 35-40: *retrieving all the attributes*) as a function of the first set (column 2, lines 24-48: *wherein the attributes are retrieved by parsing the XML tags*), wherein the second set of security settings that specify particular operations and settings for securing the messages, wherein the particular operations and settings comprise algorithms to be used in signing and encrypting the messages (column 4, lines 7-26: *XML encryption and XML signature are functions provided for by the message router and stored on a registry server*); and

means for applying the second set of security information to the message (column 2, lines 43-46: *determining security attributes to determine the operation to be performed on the message*).

**[0030]** Firstly, Applicant again notes the Examiner appears to be rejecting claim language not found in the currently pending claim. Applicant specifically refers to where the Examiner rejects "means for applying" when the claim expressly recites "steps for applying".

**[0031]** Secondly, Applicant reiterates that Sankar simply does not disclose a plurality of sets of security information. The disclosed "XML tags" do not constitute the claimed "first plurality of sets of security information", particularly if the disclosed "security attributes" are relied upon as being the claimed "second plurality of sets of security information".

**[0032]** The Examiner even appears to concede that at best what is first extracted from the XML tags is only "information" and not "security information".

**[0033]** Consequently, Sankar does not disclose all of the elements and features of this claim. Accordingly, Applicant asks the Examiner to withdraw the rejection of this claim.

*Dependent Claims 32-40*

**[0034]** These claims ultimately depend upon independent claim 31. As discussed above, claim 31 is allowable. It is axiomatic that any dependent claim, which depends from an allowable base claim, is also allowable. Additionally, some or all of these claims may also be allowable for additional independent reasons.

## Conclusion

**[0035]** In light of the forgoing amendments and remarks, early reconsideration and allowance of this application are most courteously solicited. Should the Examiner feel that a personal discussion might be helpful in advancing this case to allowance, they are invited to telephone or e-mail the undersigned.

**[0036]** In addition, it is believed that all of the pending claims have been fully addressed. However, the absence of a reply to a specific rejection, issue, or comment does not signify agreement with or concession of that rejection, issue, or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed.

**[0037]** Finally, nothing in this communication should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this communication, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

Respectfully Submitted,

Lee & Hayes, PLLC
Representative for Applicant

/Randall T. Palmer 61440/ Dated: 06/30/09

Randall T. Palmer
(randy@leehayes.com; 509-944-4761)
Registration No. 61440

Rob Peck
(robp@leehayes.com; 425-677-5750)
Registration No. 56826